115 年度資訊安全管理系統（ISMS）擴大導入委外服務勞務採購案

需求規範

壹、專案概述

一、專案名稱

115 年度資訊安全管理系統（ISMS）擴大導入委外服務勞務採購案（以下簡稱本專案）。

二、專案目標

本專案主要是由廠商提供台北海洋科技大學（以下簡稱本校）必要之顧問諮詢服務、規劃及協助擴大導入符合「ISO 27001」國際標準與高等教育深耕計畫「資安強化專章」要求的文件架構，並協助檢視與落實資訊安全管理系統相關作業與程序，以及執行資通系統滲透測試作業，強化整體資訊安全管理之能力，進而有效降低及控管資訊相關業務的安全風險。

三、專案範圍

圖資中心、教務處、學務處、總務處、研發處、國合處、進修推廣部、海事訓練部、校務研究中心、人事室、會計室、軍訓室、秘書室、體育室、航運系、輪機系、觀運系、餐管系、銀髮系、健照系、數遊系、寵物系、演藝系、新媒學程、通識中心。

四、專案期程

履約期限為：自決標次日起至 115 年 11 月 30 日止。各專案工作項目如有階段性之時程需求，請依規定完成。

貳、專案需求

一、維護資訊安全管理系統（ISMS）

(一)執行資通系統與資訊資產盤點作業

1.應於專案期限內輔導本校進行資通系統盤點分級，產出「資通系統清冊」。
2.協助本校依資訊資產管理作業規範，進行資訊資產鑑別與評價作業，並輔導與協助本校產出「資訊資產清冊」，以作為風險評鑑的基礎依據。

(二)執行風險評鑑與處理作業

1.協助本校分析資訊資產既存的威脅及潛在的問題，辨別威脅來源與脆弱點，協助針對風險評鑑中之威脅弱點項目進行檢視，計算並建議可接受風險等級，釐清風險安全控制的方向，並更新本專案「風險評鑑報告」。
2.依據風險評鑑作業結果評估適當風險控管方式，並針對不可接受之風險等級，提供因應對策，選擇適當的控制目標與控制措施，並更新本專案

「風險改善計畫表」。

(三)執行委外廠商稽核作業

廠商應協助規劃及執行本校委外廠商資訊安全稽核作業，至少選定 2 家委外廠商依 ISMS 規範進行資訊安全委外查核作業，並於完成稽核工作後輔導產製「委外廠商稽核報告」。

(四)協助召開資訊安全管理審查會議

協助本專案範圍資訊安全管理委員會進行年度資訊安全工作推動管理審查，並協助審查意見之改善。

二、執行資通系統滲透測試作業

對本校提供 1 個測試標的（IP/Domain）施作滲透測試服務，透過模擬駭客的攻擊方式，對目標主機或網路服務進行安全強度的測試，找出可能的資安漏洞，將所發現之弱點與過程詳細記錄，並提出相關安全建議及協助檢視本校修補果果。

三、執行資安健診作業

(一)資安健診之項目應包含網路架構檢視、有線網路惡意活動檢視、使用者端電腦惡意活動檢視（30 部）、伺服器主機惡意活動檢視（5 部）、目錄伺服器及防火牆連線設定檢視（各 1 部），並提出相關安全建議及協助檢視本校修補結果。

(二)進行資安健診之日期、時間應配合本校時程，並經本校同意後始得為之。

(三)執行任何會影響系統正常服務之攻擊與風險，須事先提出說明經過本校授權後才可執行，且當意外發生應協助本校業務承辦人員復原至正常狀態。

(四) 本專案所有內容及測試相關資訊不得揭露予任何未授權之第三人知悉，亦不得複委託其他廠商進行資安健診，且應採取適當及必要之保護措施，以防止第三者不當或未經授權而取得或使用。

四、檢視個人資料檔案安全維護計畫

本校已依「個人資料保護法」及「私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法」訂定個人資料檔案安全維護計畫，廠商應協助檢視是否符合相關規定及提出修訂建議。

參、專案管理

一、工作計畫書

廠商依本契約履約項目，於決標次日起 20 個工作天內，交付工作計畫書，經本校審核通過後據以執行，其內容至少應包括人力、時程、工作項目、執行規劃、專案管理、專案組織、品質管制、進度稽核點及教育訓練計畫等事項。

二、專案團隊組成

(一)廠商應通過 ISO 27001 第三方驗證，驗證範圍應涵蓋本專案之工作範圍。

(二)廠商應依本專案需求提出現有之技術人數及管理人員數，並研擬評估預計投入本專案之人數（參與本專案之專案成員至少需 4 人（含）以上)、組織架構、職責分工、人力配置與人員資歷（各人員相關之專業認證執照、相關工作資歷及技術專長應載明於工作計畫書中)。

(三)履約時應與工作計畫書中所提成員一致，專案團隊成員如有異動， 替換人員學經歷除應與被替換人員相仿外，並需於變動前 5 個工作天，提送替換理由及替換人員相關資歷資料，經本校同意後始得替換。

(四)專案團隊成員中應指定專案經理 1 人、資訊安全輔導顧問 2 人、資訊安全技術顧問 1 人。並符合下列規定：

職務名稱	負責事項	資格條件
專案經理	負責整體規劃、任務分派、進度控管、作業協調等管理工作。	1.具備實際擔任ISO 27001資訊安全管理系統輔導專案經理經驗。 2.具資安責任等級B級（含）以上機關ISMS 輔導7年（含）以上經驗；須於工作計畫書中列表說明並提供相關佐證資料供查驗。 3.須具備ISO 27001主導稽核員、BS 10012主導稽核員、ISO 27701主導稽核員、ISO 27017主導稽核員、ISO 27018主導稽核員、ISO 22301主導稽核員、CISSP、CISM及PMP等證照。
資訊安全輔導顧問	1.本專案執行者，辦理本專案相關活動。 2.參加專案檢討會，報告專案執行情形。	1.具備實際擔任ISO 27001資訊安全管理系統輔導顧問經驗。 2.具備實際參與大專院校之資訊安全管理系統建置及輔導經驗，須於工作計畫書中列表說明並提供相關佐證資料供查驗。 3.須具備ISO 27001主導稽核員證照、ISO 27701主導稽核員證照。
資訊安全技術顧問	協助提供資安技術檢測服務	1.具備2年（含）以上資安技術檢測經驗，須於工作計畫書中列表說明並提供相關佐證資料供查驗。 2.須具備ISO 27001主導稽核員證照。

(五)所有資格證明文件，廠商應據實提報，如有偽造，廠商自負相關法律責任。

三、專案管理

(一)專案進行期間，廠商對於專案之進度與品質應建立監控方法，以期有效解

決問題與異常狀況，並明確說明雙方應配合與協調之事實。

(二)專案團隊成員需簽署保密同意書與保密切結書，並於專案啟動會議前交付本校確認。

(三)專案成員若因故請假或離職時，廠商應指派代理人代理且須經本校同意，廠商所指派之代理人不得由本專案成員兼任,且其資歷應與被代理人相當。

(四)專案成員如有服務不佳或違反本校相關規定等之情形，本校得提出更換人員要求，廠商應予配合，並須於本校通知日起 1 週內遞補同等資歷人員，且須經本校同意。

(五)廠商須依本校需求定期與本校召開專案會議，會議之目的在檢討專案執行狀況,明定未確定之事項,解決發生之問題,討論雙方應配合及協調事項，廠商應由資訊安全輔導顧問及主要工作人員參與會議。資訊安全輔導顧問應於會議前 3 日提出專案工作報告,內容應包括專案工作進度、未來工作事項、雙方應配合與協調事項等項目，並留存會議紀錄備查。

(六)其他注意事項

1.專案期間自本校取得之資料，於專案結束後交還，不得複製、轉載或引用。

2.專案產出之各項文件屬本校之著作財產，非經本校正式書面同意，不得轉載或引用。

3.廠商應事前與本校充分溝通，確實瞭解本校需要，得標後不得以資訊不足為由，延誤進度。

4.如發生執行時程落後，本校得要求廠商增加參與本專案人力，以便儘速趕上本專案預期進度。

5.廠商須協助本校相關同仁了解資訊安全管理規範標準、撰寫標準文件流程及協助溝通本專案進行時所發生之衝突。

四、交付項目及工作時程

(一)各項交付日期依據實際執行情形經本校核准後可酌予調整，惟最後交付項目時間仍不得逾 115 年 11 月 30 日。

(二)各項交付項目文件均為 1 式 2 份,以 A4 尺寸紙張直式橫書雙面製作印刷，並裝訂成冊，文書之電子檔並應儲存於光碟片 1 式 2 份。

(三)專案各階段交付項目及工作時程如下表所示：

階段	階段內容	交付項目	交付日期
1	提交 工作計畫書	1.工作計畫書。 2.完成保密同意書、保密切結書簽訂。	決標日次日起 20個工作天內
2	維護資訊安全管理系統 （ISMS）	1.資通系統清冊、資訊資產清冊。 2.風險評鑑報告、風險改善計畫表。	115年08月31日前
		委外廠商稽核計畫、委外廠商稽核報告。	115年09月30日前
		管理審查會議簡報、會議紀錄。	115年11月30日前
3	執行資通系統滲透測試作業	滲透測試報告（初測、複測）	115年10月31日前
4	執行資安健診作業	資安健診報告（初測、複測）	115年10月31日前
5	檢視個人資料檔案安全維護計畫	個人資料檔案安全維護計畫修訂建議	115年11月30日前

(四)專案各階段應完成約定之交付文件，並經驗收合格後，始辦理該階段款項給付；本專案款項支付共分為五階段辦理。